ABSTRACT OF THE DISCLOSURE

A long-lived broadcast encryption method that adapts to the presence of compromised keys and continues to broadcast securely to privileged sets of users over time. In one aspect, a method for providing long-lived broadcast encryption comprises the steps of: allocating, to each of a plurality of subscribers, a corresponding set of subscriber keys; broadcasting encrypted content to the plurality of subscribers using a set of broadcast keys, wherein the encrypted content is decoded by a given subscriber using the subscriber's corresponding set of subscriber keys; modifying the set of broadcast keys, which are used for broadcasting encrypted content, by excluding compromised subscriber keys; and updating a set of subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below a first predetermined threshold. In a long-lived broadcast encryption scheme, for any positive fraction β, a plurality of parameter values may be selected, *a priori*, in such a way to ensure that a steady state is achieved wherein, at most β of the total number of issued cards need to be replaced in a given recarding session.